

CLAIMS

What is claimed is:

- Sub
a1
- 5
- 10
- 15
- 20
1. A method in a distributed system, comprising the steps of:
downloading code from a server;
determining a set of constraints to implement secure communication with
the server; and
using secure code to verify that the downloaded code will enforce the set
of constraints when the downloaded code is used to communicate with the
server.
 2. The method of claim 1, further comprising the step of:
using the downloaded code to invoke a method on the server, wherein the
downloaded code enforces the set of constraints on the server.
 3. A method in a distributed system for ensuring trustworthiness of a first
proxy, comprising the steps of:
downloading the first proxy containing code for communication purposes;
using the first proxy to obtain a second proxy containing code for
communication purposes;
determining whether the second proxy is trustworthy by using a
trustworthiness verification routine;

requesting the server to determine whether the first proxy is trustworthy by using the second proxy when it has been determined that the server is trustworthy; and

4. The method of claim 3, wherein the requesting step further comprises the substeps of:

```

receiving codebase information and signer information for the trust
verifier from the server;

```

when it has been determined that the trust verifier routine is trustworthy, using the trust verifier routine to determine whether the first proxy is trustworthy.

5. A method for establishing trust in a proxy containing code downloaded from a server, comprising the steps of:

determining whether the proxy is an instance of a trusted proxy class;

verifying at least one component of the proxy when it has been

determined that the proxy is an instance of the trusted proxy class, wherein the verifying step comprises the substeps of:

verifying trust in an invocation handler of the proxy;

determining whether the proxy has an activator; and

verifying the trustworthiness of the activator, when it has been

determined that the proxy has an activator; and

using the proxy to invoke a method on the server when it has been

determined that the proxy is an instance of the trusted class and the at least one component of the proxy has been verified successfully.

6. A method for establishing trust in a proxy containing code downloaded from a server, comprising the steps of:

determining whether the proxy is an instance of a trusted proxy class;

verifying at least one component of the proxy when it has been

determined that the proxy is an instance of a trusted proxy class, wherein the

proxy has an invocation handler and a plurality of socket factories, and wherein

the verifying step comprises the substeps of:

obtaining the invocation handler from the proxy;

5

10

15

authenticating the activator, when it has been determined that the proxy has an activator, wherein the authenticating step further includes the substeps of:

using the activator verifier to determine whether the activator is trusted by the server; and

is not trusted by the server; and

20

a server computer, comprising:

24

a processor that runs the service; and
a client computer, comprising:

a memory with a proxy that facilitates use of the service, a client
program that invokes a method of the service using the proxy, and a secure
verifier that can be used to verify that the proxy will enforce security constraints
when communicating with the service; and
a processor that runs the client program.

8. The distributed system of claim 7, wherein the server computer and the
client computer communicate via the Internet.

9. The distributed system of claim 7, wherein the server computer and the
client computer communicate via a local area network.

10. The distributed system of claim 7, wherein the security constraints are set
by the client program.

11. The distributed system of claim 7, wherein the security constraints are set
by the service.

5
10
15

10

152

20

26

using the first proxy to invoke a method on the server when it has been determined that the first proxy is trustworthy, that the second proxy is trustworthy, and that the server is trustworthy.

[illegible]